Refine Search

Search Results -

Terms	Documents
L16 and (change or modify or modificat$ or modification)	165

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search:

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Wednesday, December 14, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L17	L16 and (change or modify or modificat$ or modification)	165	L17
L16	l15 and(dissatisfied or dissatifi$) and customer	169	L16
L15	(credit and account and "credit card")	23331	L15
L14	L13 and (dissatisfied or dissatifi$) and customer	2	L14
L13	L12 and (change or modify or modificat$ or modification)	336	L13
L12	l4 and (credit and account and "credit card")	360	L12
L11	L10 and offer not ("credit account" and "credit card account")	788	L11
L10	(credit and delinquent or overdue or past adj due) not ("credit account" or "credit card account") and (parameter or value) and (modificati$ or change or modify or modification) and offer	788	L10
L9	l1 and (credit and delinquent or overdue or past adj due) not ("credit account" or "credit card account") and (parameter or value) and (modificati$ or change or modify or modification) and offer	0	L9

L8	l1 and (credit and delinquent or overdue or past adj due) not ("credit account" or "credit card account") and (parameter or value) and (modificati$ or change or modify or modification) and offer not ("credit account" and "credit card account")	0	L8
L7	(credit and account and "credit card") and (change near modificat$ or change near modiifcation)	2519	L7
L6	705.clas.	38446	L6
L5	705/39	1730	L5
L4	705/38	925	L4
L3	705/35	2229	L3
L2	4346442.pn.	2	L2
L1	5933817.pn.	2	L1

END OF SEARCH HISTORY

L17: Entry 164 of 165 File: USPT Oct 18, 1994

US-PAT-NO: 5357563
DOCUMENT-IDENTIFIER: US 5357563 A

TITLE: Data card terminal for receiving authorizations from remote locations

DATE-ISSUED: October 18, 1994

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Hamilton; James H.	Lawrenceville	GA		
Cavicchi; Peter R.	N. Babylon	NY		
Depew; Timothy W.	Ft. Lauderdale	FL		
Friedman; Shelley K.	Boca Raton	FL		
Kligfeld; Edward G.	Ft. Lauderdale	FL		
Noblett, Jr.; Paul W.	Ft. Lauderdale	FL		
Vogt; Diane T.	Sunrise	FL		
Stills; James T.	Atlanta	GA		
Philmon; Gregory A.	Loganville	GA		
Nair; Parameswaran B.	Acworth	GA		
Morton; Murray A.	Coral Springs	FL		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
MicroBilt Corporation	Atlanta	GA			02

APPL-NO: 08/079501 [PALM]
DATE FILED: June 17, 1993

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATION This application is a division of application Ser. No. 07/820,401, filed Jan. 10, 1992, entitled DATA CARD TERMINAL WITH EMBOSSED CHARACTER READER AND SIGNATURE CAPTURE, which discloses subject matter in common with application Ser. No. 08/148,831, filed Nov. 5, 1993, entitled SYSTEMS AND METHODS FOR OPERATING DATA CARD TERMINALS FOR TRANSACTION CHARGEBACK PROTECTION, which is a division of application Ser. No. 07/819,327, filed Jan. 10, 1992, entitled SYSTEMS AND METHODS FOR OPERATING DATA CARD TERMINALS FOR TRANSACTION CHARGEBACK PROTECTION.

INT-CL: [05] H04M 11/00

US-CL-ISSUED: 379/91; 379/221, 235/380
US-CL-CURRENT: 379/91.01; 235/380

FIELD-OF-SEARCH: 379/91, 379/111, 379/114, 379/115, 379/144, 379/155, 379/67, 379/88, 379/89, 379/213, 379/214, 379/218, 379/221, 379/207, 235/375, 235/380-382.5

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3727186	April 1973	Stephensen, Jr. et al.	
☐	3787623	January 1974	Stephensen, Jr.	
☐	3885108	May 1975	Zock	
☐	3938090	February 1976	Borison et al.	
☐	4017835	April 1977	Randolph	379/91
☐	4028733	June 1977	Ulicki	
☐	4054756	October 1977	Comella et al.	379/207
☐	4071697	January 1978	Bushnell et al.	
☐	4109238	August 1978	Creekmore	
☐	4119815	October 1978	Frankfort et al.	379/221
☐	4139739	February 1979	Von Meister et al.	379/207
☐	4187498	February 1980	Creekmore	
☐	4439636	March 1984	Newkirk et al.	
☐	4489438	December 1984	Hughes	
☐	4525712	June 1985	Okano et al.	
☐	4587379	May 1986	Masuda	379/91
☐	4625276	November 1986	Benton et al.	
☐	4630201	December 1986	White	
☐	4634845	January 1987	Hale et al.	
☐	4672377	June 1987	Murphy et al.	
☐	4689478	August 1987	Hale et al.	
☐	4707592	November 1987	Ware	
☐	4710955	December 1987	Kauffman	
☐	4724521	February 1988	Carron et al.	
☐	4734858	March 1988	Schlafly	
☐	4788420	November 1988	Chang et al.	
☐	4796292	January 1989	Thomas	
☐	4822985	April 1989	Boggan et al.	
☐	4897865	January 1990	Canuel	
☐	4908850	March 1990	Masson et al.	
☐	4951308	August 1990	Bishop et al.	
	4972461	November 1990	Brown et al.	

☐				
☐	4972463	November 1990	Danielson et al.	
☐	4975942	December 1990	Zebryk	
☐	4988849	January 1991	Sasaki et al.	
☐	5007084	April 1991	Materna et al.	
☐	5128983	July 1992	Tanaka	
☐	5136633	August 1992	Tejada et al.	
☐	5144649	September 1992	Zicker et al.	
☐	5239573	August 1993	Rangan	379/88

OTHER PUBLICATIONS

Perdue et al., "Conversant.RTM. 1 Voice System: Architecture and Applications", AT&T Technical Journal, Sep./Oct. 1986, vol. 65, No. 5.

ART-UNIT: 268

PRIMARY-EXAMINER: Chan; Wing F.

ATTY-AGENT-FIRM: Jones & Askew

ABSTRACT:

A data card terminal, such as a credit card transaction terminal, is disclosed. The terminal is capable of requesting and receiving electronic authorization indicia via alternative communications links. The terminal includes first communications means for automatically connecting the terminal with a transaction processing host computer system via a first communications link, and second communications means for automatically connecting the terminal with the transaction processing host computer system via a separate second communications link if the first link fails. A third communications means automatically connects the terminal to an audio response unit (ARU) via a third communications link in response to a "call me" signal from the host computer system, or if the first and second communications links fail. Transaction data is automatically transmitted from the terminal to the ARU via DTMF signals. The terminal includes means for receiving manual entry of audible authorization indicia received from the ARU, and means for verifying manually entered authorization indicia.

41 Claims, 43 Drawing figures

Previous Doc Next Doc Go to Doc#

L17: Entry 164 of 165 File: USPT Oct 18, 1994

DOCUMENT-IDENTIFIER: US 5357563 A
TITLE: Data card terminal for receiving authorizations from remote locations

Abstract Text (1):
A data card terminal, such as a credit card transaction terminal, is disclosed. The terminal is capable of requesting and receiving electronic authorization indicia via alternative communications links. The terminal includes first communications means for automatically connecting the terminal with a transaction processing host computer system via a first communications link, and second communications means for automatically connecting the terminal with the transaction processing host computer system via a separate second communications link if the first link fails. A third communications means automatically connects the terminal to an audio response unit (ARU) via a third communications link in response to a "call me" signal from the host computer system, or if the first and second communications links fail. Transaction data is automatically transmitted from the terminal to the ARU via DTMF signals. The terminal includes means for receiving manual entry of audible authorization indicia received from the ARU, and means for verifying manually entered authorization indicia.

Brief Summary Text (2):
The present invention relates generally to data card transaction systems that use terminals such as credit card transaction terminals, and relates more particularly to a data card transaction terminal that detects the physical presence of a data card with an embossed character reader and a magnetic stripe reader, provides signature capturing capability, and may be utilized in transaction information processing systems for conducting transactions that are chargeback protected to a merchant utilizing the terminal.

Brief Summary Text (4):
The use of data cards or payment cards, such as credit cards, has gained widespread acceptance as a method of paying for goods and services. As used herein, the term "data card" will be generally used to signify such cards, which can include credit cards, debit cards, and other financial account cards. Data cards in use today typically include a magnetic stripe containing account and other information, and most often include an account number and other information in embossed or raised characters.

Brief Summary Text (5):
Two elements must be present before a credit card transaction can be completed successfully. First, the consumer or cardholder must possess a valid credit card. Second, the merchant must be authorized to accept the card as payment for the goods or services and to receive payment from the organization that issued the credit card. The card issuing organization subsequently receives payment from the cardholder.

Brief Summary Text (6):
Credit cards are issued by banks and other financial organizations, generally as members and under the regulations of a credit card issuing association or entity. VISA.RTM., MasterCard.RTM., DISCOVER CARD.RTM., and AMERICAN EXPRESS.RTM. are examples of credit card issuing associations or entities for particular brands of

data cards. When a credit card is issued, the issuer is, in effect, granting a line of credit to the cardholder. Because the issuer is granting a line of credit, a credit card will be issued only after the issuer has conducted a credit background check and is satisfied as to the cardholder's ability and willingness to repay the debts incurred. The issuer's confidence is reflected in the amount of credit granted, which may range from a few hundred dollars to tens of thousands of dollars.

Brief Summary Text (7):
Many data card transactions involve third-party credit card transaction processors in addition to the merchant and credit card issuer. Transaction processors, which are sometimes independent business institutions, provide merchants with data processing services that facilitate the flow of credit card transaction data and the corresponding payments of monies between the merchants and card issuers. The flow of transaction data from the merchant to the issuer via a transaction processor is commonly referred to as "processing" or "clearing" the transactions. The flow of money from the issuer to the merchant via a processor is known as "settlement". The term "transaction processor", as used herein, generally means a third-party institution that processes card transactions independently of a card issuer, but can also include card issuers and card issuing associations that process their own transactions.

Brief Summary Text (8):
In a typical credit card transaction, a card holder presents a credit card to a merchant, who records transaction data by using either an electronic terminal or a manually imprinted sales draft. The recorded data includes the amount of the purchase, the cardholder's account number, the card's expiration date, the merchant identification number, and the date of the transaction. In most cases, the cardholder is also required to sign a copy of the receipt.

Brief Summary Text (9):
At the end of each day, the merchant determines the total dollar volume of the credit card transactions completed and prepares a deposit slip indicating that amount. All of the transaction data is then transferred to the merchant's credit card transaction processor and entered into the transaction processor's computers. This transfer may be electronic, in which case a data capture terminal transfers the data directly to the processor's computer. Alternatively, the transfer may involve the deposit of imprinted paper sales drafts and subsequent entry of the data into the computers by the processor's data entry personnel.

Brief Summary Text (10):
Once the data is received by the transaction processor, the amount of the merchant's "deposit" is verified and recorded. At that point, the transactions are separated according to the type of credit card used to complete the transaction. The transaction processor then transfers the corresponding transaction data to the appropriate credit card issuer or card issuing association. After the data is transferred to the issuer, the issuer posts the individual transactions to the appropriate cardholder's account.

Brief Summary Text (12):
As a part of transaction settlement, transaction processors and issuers assess fees for processing the credit card transaction. These fees are commonly referred to as the "discount rate" and are usually calculated as a percentage of the face value of the credit card transaction. The issuer deducts its fee as percentage from the total amount due the transaction processor.

Brief Summary Text (13):
Although credit cards provide significant convenience for both cardholders and merchants, there are also well known risks associated with credit card transactions. The principal risk is loss resulting from fraudulent or unauthorized

use of the credit card. In such a case, the goods or services are taken by the cardholder and are usually unrecoverable. The loss must then be absorbed by the merchant, credit card transaction processor, and/or the credit card issuer.

Brief Summary Text (14):
Over the years, card issuers and merchants have relied on several different methods to protect themselves from fraud or misuse and to verify the validity of a credit card before completing a transaction. Initially, the card issuers provided "warning bulletins" to merchants. Warning bulletins, which are still in widespread use, are booklets that list the account numbers of credit cards that should no longer be accepted. Account numbers are included on these lists if the card has been reported stolen, if the cardholder has exceeded his or her credit limit or has become delinquent in the payments to the issuer, or if a card should not be accepted for another reason (such as mistakenly issued cards and cards that are invalid outside their country of origin).

Brief Summary Text (15):
More recently, card issuers and card issuing associations have provided real-time access to their computerized databases. This allowed merchants to request telephonic authorization for a transaction based on a search of a continually updated database before completing each transaction. For a typical transaction authorization, the merchant obtains an "authorization code" or authorization indicia from an authorization source or institution, often via telephone. Authorization sources include card issuing associations, card issuers themselves, as well as independent credit card transaction processors that also provide clearing and settlement services between merchants and card issuers.

Brief Summary Text (17):
Some transaction processors and card issuers provide electronic terminals that read the account number and expiration date from a magnetic stripe on the credit card. Once the merchant enters the purchase amount into the terminal, the terminal automatically dials an authorization source host computer and initiates an authorization request. The terminal displays and/or stores an approval code (authorization indicia) if the transaction is authorized. In each case, the approval code is recorded along with the other transaction data.

Brief Summary Text (22):
A "chargeback" occurs when a credit card issuing association refuses to honor a presentment of a processed transaction because the issuer believes it violates a specific operating regulation. The chargeback results in reversal of the transaction to the transaction processor or merchant. Some transaction processors provide research services on behalf of their customers/merchants in an effort to resolve the dispute to the benefit of the merchant and re-present the transaction to the issuer for payment. Chargebacks are allowed only under specific conditions as provided in the association's operating regulations, and can be resolved or reversed only under specified conditions.

Brief Summary Text (24):
Disputes regarding transaction procedures can be further classified to include authorization-related disputes, retrieval-related disputes, and transaction data disputes. Authorization related disputes are usually initiated by the card issuer when the credit card account is in a delinquent, over limit, or otherwise allegedly uncollectible condition, and the issuer cannot locate a record indicating that the transaction was authorized. The premise for the dispute is that the issuer claims the transaction would not have been authorized if the merchant had properly sought authorization at the time of the transaction.

Brief Summary Text (25):
Retrieval-related disputes can be initiated by a cardholder or by a card issuer. These disputes commonly arise when a cardholder sees an unfamiliar transaction

posted to his or her account. At that point, the cardholder is entitled to request, through the issuer, a copy of the paper documentation supporting the transaction. In other situations, the card issuer may request copies to aid in its research of disputes or fraud. Such requests are called "retrieval requests." Once the cardholder or issuer properly requests a copy of the documentation, the transaction may be charged back to the transaction processor or merchant if the requested documentation is not provided within a prescribed time limit. A transaction can also be charged back when the copy of the transaction provided is of poor quality or legibility, or does not include the minimum information required by the card issuer's regulations.

Brief Summary Text (26):
Transaction data disputes typically occur when there are problems associated with the cardholder's account number, the amount of the purchase, the signature, the date of the transaction, the validity of the card on the date of the transaction, etc. Such problems may occur when any of the above data are improperly entered or illegible. These disputes are commonly referred to as "technical" disputes or chargebacks, since they are based on errors in merchant procedures or in the entry of the data.

Brief Summary Text (27):
Cardholder disputes occur when the cardholder denies participation in the transaction, or where the cardholder is dissatisfied with the merchandise or services purchased. In these cases, federal laws provide a cardholder with certain consumer rights. Cardholder disputes may also include claims that a single transaction was processed more than one time, that a credit issued by the merchant to the cardholder was not processed, or that the cardholder had revoked a merchant's authority to charge his account.

Brief Summary Text (29):
In recent years, several devices and services have been created in order to simplify the storage and retrieval of transaction data, and to reduce the likelihood of authorization-related and technical chargebacks by insuring the accuracy of the recorded transaction data. So-called electronic "data capture" data card transaction terminals electronically detect and decode the cardholder's account number and expiration date from the magnetic stripe, and receive a purchase amount from a keypad. Once the data is entered in this fashion, it is used to print a receipt and is electronically transmitted to a transaction processor.

Brief Summary Text (31):
Some third party credit card transaction processors market their authorization, processing, and settlement services to merchants in conjunction with a "chargeback defense system" of some sort. The chargeback defense systems promoted by some processors include a review of chargeback against the operating regulations promulgated by card issuing associations. In addition, some transaction processors maintain databases of transaction information that allow the processor to obtain reversal of certain types of chargebacks on behalf of its customers/merchants. For example, if an issuer refuses to honor a transaction because it is unable to locate an authorization record, the processor may be able to reverse the chargeback without involving the merchant by providing the missing record of authorization to the issuer.

Brief Summary Text (33):
It is possible that data card transactions where a card is physically presented by a card holder to a merchant and the account number is electronically obtained are more likely to be valid transactions of the card holder than transactions where the account number was manually entered at a keyboard. If it were possible to compare and verify the account number, expiration date, or other information obtained from reading the magnetic stripe of a data card against another source of information associated with the card (such as the embossed characters on the data card or a

second track of information on the magnetic stripe), it would be even easier to verify that a card was physically present for the transaction. It would then be possible to provide credit card issuers and/or transaction processors with greater assurance that a data card was indeed physically present at a transaction terminal on a given date in connection with a given transaction. Such greater assurances could therefore provide an incentive to a transaction processor or other entity to guarantee such transactions and make them "chargeback protected" for the merchant.

Brief Summary Text (37):
The Tasaki et al. patent provides little useful information as to how the pattern detection is actually accomplished. It appears that the device merely detects a simple geometric pattern of raised areas embossed on the card instead of embossed characters, since there is no discussion that the pattern is encoded with information such as account number, name, expiration date, or the like. Moreover, the movement of the card past the linear array of sensors requires a special mechanism to move and handle the card. It would be more useful and efficient in data card applications if the embossed character region, which in credit cards contains name, account number, expiration date, etc., could be read and decoded to obtain the information encoded therein, without a complex card moving mechanism.

Brief Summary Text (38):
U.S. Pat. No. 5,055,838 describes a capacitive silicon tactile imaging array comprising a matrix of sensors and a method of making same. Such devices might be employed for taking an electronic "picture" of the embossed character regions provided on many current data cards; this picture conceivably could be used in verifying the account information provided in the magnetic stripe of the data card. However, such an electronic "picture" requires many digital signals to represent, resulting in large memory storage requirements and processing delays to handle the large amounts of data. In addition, it is a non-trivial problem to adapt a matrix sensor for making such an electronic picture of the embossed area of a card and accurately determining, with a computer or other electronics, what characters are present in the embossing on the card.

Brief Summary Text (45):
As is known, card identifying information in present day data cards is provided in a plurality of sources on the data card, for example, the account number and other information is provided on a plurality of tracks on a magnetic stripe on the card, and the account number, cardholder name, and expiration date are typically embossed on the card. According to another aspect of the invention, the card identifying information obtaining means comprises means for obtaining the card identifying information from a first source of the plurality of sources and from a second source of the plurality of sources. Means are provided for verifying the accuracy of card identifying information obtained from the first source. And, means are provided for restoring at least a portion of the card identifying information obtained from the fast source with information obtained from the second source in response to a determination by the verifying means that the card identifying information obtained from the first source is not accurate or complete.

Brief Summary Text (47):
The preferred verifying means comprises means for computing the longitudinal redundancy check (LRC) associated with a track on the magnetic stripe, and the restoring means is operative for restoring at least a portion of the account number read from the magnetic stripe reader with at least a portion of the account number read from the embossed card reader. Alternatively, the verifying means may comprise means for checking a checksum associated with the account number.

Brief Summary Text (52):
Yet another aspect of the inventions relates to methods of operation of a transaction processor that receives transaction information from a merchant utilizing a terminal constructed in accordance with the present invention. The

method relates to guaranteeing a financial transaction conducted by a cardholder utilizing a data card against chargebacks of the transaction to a merchant participating in the transaction. The disclosed method includes the step of providing to the merchant a data card transaction terminal. At the terminal, and in response to the presentation of a data card by a cardholder in connection with a proposed transaction, the method comprises automatically detecting the physical presence of the data card at the terminal, automatically detecting an account number associated with the data card, and capturing a signature of the cardholder in connection with the transaction.

Brief Summary Text (57):
According to yet another aspect of the invention, there is disclosed a method of obtaining authorization indicia from an authorization source, preferably carried out by a data card terminal. The method comprises establishing a communication link with a transaction processing host computer system. Once the communication link is established, the terminal provides the detected account number associated with the data card to the transaction processing host computer system, and provides a proposed transaction amount to the transaction processing host computer system.

Brief Summary Text (58):
The method further comprises, at the transaction processing host computer system, attempting to establish a communication link to an authorization source computer system corresponding to the card presented. The transaction processing host computer system, in response to establishment of the communication link with the authorization source computer system, provides the detected account number associated with the data card and the proposed transaction amount to the authorization source computer system.

Brief Summary Text (71):
More particularly described, a preferred system for providing authorizations in connection with data card transactions includes a data card terminal comprising means for detecting an account number associated with a data card presented by the cardholder in connection with a proposed transaction, a first communication means for connecting the terminal for data communications via a first telecommunications link, a second communications means for connecting the terminal for data communications via a separate second telecommunications link in the event of failure to establish communications via the first telecommunications link, and a third communications means for connecting the terminal for communications via a separate voice grade third telecommunications link in the event of failure to establish communications via the first telecommunications link or the second telecommunications link.

Brief Summary Text (77):
The preferred terminal further comprises means for detecting an account number associated with the data card presented by the cardholder in connection with the proposed transaction, and means for automatically providing the detected account number to said transaction processing host computer system or said ARU, in the manner described in connection with other preferred embodiments. The preferred account number providing means comprises signal means for providing the detected account number to the transaction processing host computer system, and DTMF means for providing the detected account number to said ARU.

Brief Summary Text (84):
It is a further object of the present invention to provide an improved apparatus and method by which a credit card transaction terminal will ensure that all data related to a transaction is collected before the transaction is completed.

Brief Summary Text (89):
It is a further object of the present invention to provide improved systems for use in handling data card transactions that will allow a credit card transaction

processor to respond to retrieval requests without the involvement of the merchant.

Drawing Description Text (2):
FIG. 1 provides an overview of a prior art credit card transaction processing system.

Drawing Description Text (3):
FIG. 2 illustrates a credit card transaction processing system that employs a data card transaction terminal constructed in accordance with the preferred embodiment of the present invention.

Drawing Description Text (27):
FIG. 26 is a flow diagram illustrating a preferred subroutine for conducting a credit card transaction with card detection, transaction authorization, and signature capture forming a part of the transaction terminal/printer software method of FIG. 25.

Detailed Description Text (5):
A "data card" can mean a debit card, a credit card, or other financial account card. Such data cards typically have a magnetic stripe associated with the card, carrying an account number associated with the card, expiration date, issuing institution, and other information, as well as a visible indication of an account number and other information in an area of embossed characters. The terms "data card", "credit card", etc. are used interchangeably herein.

Detailed Description Text (8):
A "transaction processor" is an institution that processes data card transactions, for example a credit card transaction processing company. Transaction processors are sometimes independent third party institutions that are not related to any particular credit card issuer. However, since many card issuing associations and card issuers also process transactions, card issuing associations and card issuers are generally included within the term "transaction processor", except where a distinction between the institutions is required.

Detailed Description Text (9):
A "card issuing association" or entity, as used herein, is an institution or other entity that issues regulations governing a particular brand of data card, for example VISA.RTM., MasterCard.RTM., AMERICAN EXPRESS.RTM., DISCOVER.RTM., and the like. Some associations called "bankcard associations" typically comprise "member banks" that actually issue the credit cards, for example VISA.RTM. and MasterCard.RTM. bankcard associations. Other non-bank entities such as AMERICAN EXPRESS.RTM. are included within the term for purposes of this invention. Card issuing associations typically accumulate transaction data from transaction processors and send it to the individual cardholder's bank.

Detailed Description Text (10):
A "card issuer", as used herein, is an institution or organization, often a bank, that issues a data card such as a debit or credit card. Card issuers are generally members of a card issuing association. However, the terms "card issuer" and "card issuing association" are sometimes used synonymously when the context suggests an entity that is responsible for issuance and/or regulation of transactions involving certain data cards.

Detailed Description Text (12):
"Clearing" a transaction refers to the process by which data pertaining to a merchant's credit card transactions is transferred to a card issuer. Transaction clearance is often provided nowadays by transaction processors that are independent of credit card issuers. However, since card issuers also clear transactions themselves, they are often transaction processors as well.

Detailed Description Text (14):
"Referral" means a signal or predetermined indicia received by a merchant from an authorization source indicative that the merchant should contact the authorization source, or a card issuer, in connection with a particular transaction. A referral is often generated in response to a determination that a transaction should not be completed because the account associated with a presented card is over its credit limit, may have been stolen, or for some other reason.

Detailed Description Text (16):
An "audio response unit" or "ARU" is a synthesized voice generating apparatus that responds to dual tone multiple frequency (DTMF) signals provided by standard TOUCH-TONE.RTM. telephones to enter the account number, expiration date and purchase amount. In addition, the ARU contains circuitry that is capable of recognizing certain spoken words and numbers. If a transaction is approved, the ARU's voice synthesizer provides an approval number and is operative for generating an audible but synthesized voice message corresponding to a predetermined message. For example, an ARU may be programmed to provide messages such as, "Transaction authorized, approval code is 12345", or "Transaction declined, call me." Such messages are generated and delivered to merchants automatically and telephonically, without human intervention or participation.

Detailed Description Text (18):
General Description of Credit Card Transaction Processing Systems

Detailed Description Text (19):
FIG. 1 illustrates generally a typical prior art system 8 used to process and settle data card transactions. The system 8 is known in the art, and is subject to many of the difficulties to which the present inventions are addressed. The system 8 contemplates that a transaction processor 12 (which could be a card issuer or an independent transaction processor) is employed for transaction clearing and settlement. A merchant 13 may transfer transaction data to the transaction processor 12 electronically or in the form of paper sales drafts. The data is typically transferred from the transaction processor to the credit card issuer electronically. Once the card issuer receives the data, the transactions are posted to the appropriate cardholder's account or stored for subsequent posting to the appropriate cardholder's account. Settlement occurs as funds are transferred from the issuing institution to the merchant.

Detailed Description Text (20):
In a typical transaction, a cardholder proposes to purchase goods or services and presents a credit card, such as one of the types 15a-d, to the merchant 13 as the method of payment. In some cases, the merchant communicates with the transaction processor 12 as an authorization source in order to have the proposed transaction authorized prior to completing the transaction. In other cases, the merchant communicates with a separate authorization source 17 for requesting transaction authorization. Either authorization source may communicate with a card issuing association 18 or a card issuer 19 for authorization.

Detailed Description Text (22):
The merchant 13 in the system 8 uses an electronic terminal 16 or manual imprinter to record the data pertaining to the transaction. The recorded data includes the account number and expiration date shown on the card, the amount and date of the purchase, the authorization number (if the proposed transaction is approved), and the cardholder's signature.

Detailed Description Text (23):
Periodically (e.g., daily), the merchant transfers the data from all of the credit card transactions to the transaction processor 12 so that the transactions may be processed or "cleared". Some transaction processors handle transactions for

different types of credit cards, thereby obviating the merchant's need to communicate separately with different card issuers. In such cases, the transaction processor 12 separates that merchant's transactions according to the type of card used. The transaction processor then combines the transactions for each type of card with those received from other merchants and forwards the data to the respective credit card issuing association 18a-d.

Detailed Description Text (24):
In the case of VISA.RTM. and MasterCard.RTM. card issuing associations, the entities that receive the data from the transaction processor 12 comprise associations 18a-b that are formed by "member banks" 19a-b that actually issue the credit cards. These associations 18a-b accumulate the data and send it to the individual cardholder's bank. In the case of other credit card issuing associations, e.g., DISCOVER.RTM. 18c and AMERICAN EXPRESS.RTM. 18d, the transaction processor 12 transmits data directly to the credit card issuing association. In either case, once the entity that issued the credit card to the cardholder receives the data, each transaction is posted to the appropriate account and a statement or bill 21a-d is subsequently sent to the cardholder.

Detailed Description Text (26):
Preferred Credit Card Transaction Processing System Employing Present Invention

Detailed Description Text (27):
FIG. 2 illustrates a preferred data card transaction processing system 25, implemented as a credit card transaction processing system, that incorporates the present inventions, including a data card terminal/printer 30 constructed as described herein. In the preferred system 25, the cardholder purchases goods or services and presents a credit card 15a, for example a VISA card, to the merchant as the form of payment, as in the system 8.

Detailed Description Text (28):
At that point, the merchant uses the preferred data card transaction terminal/printer 30, which includes a transaction terminal 35 and a signature capture printer 38, to record the transaction data. More particularly, the terminal 35 reads the account number and expiration date directly from the card by means of a card swipe interface, and may also obtain information from an embossed card reader. The transaction terminal 35 thereby detects the physical presence of the data card at the terminal, and provides a "card present" signal. The terminal then prompts the merchant to enter the purchase amount via the keyboard. Once the purchase amount is entered, the printer 38 prints a portion of a paper receipt and the transaction terminal 35 prompts the merchant to have the cardholder sign the receipt. The signature capture printer 38 digitizes the signature and transmits the digitized value to the terminal 35, where data signals representative of the signature are processed and stored along with other data pertaining to the transaction. This process is described in more detail below.

Detailed Description Text (36):
If the telecommunication link with the authorization source (via host computer 40) is successful, the terminal 35 transmits certain predetermined transaction data to the host computer 40. The host computer 40 then relays the transaction data to a credit card issuing institution 18a, for example a VISA.RTM. card association, in order to receive authorization. If the transaction is authorized, an authorization code or indicia 60 is relayed from the credit card issuing institution 18a (or other authorization source) to the host computer 40, and from the host computer to the transaction terminal 35. The host computer 40 stores the transaction data and signature in a data storage facility 64. The terminal 35 also stores all of the transaction data (except the signature in the preferred embodiment, which is not retained in the terminal since the signature is transmitted to the host during the authorization communications session.

Detailed Description Text (37):
As in the general credit card transaction processing system 8 described in conjunction with FIG. 1, the transaction processor 12 separates the transaction data according to the type of card used and periodically transfers the data to the credit card issuing institution 18a, which in turn relays it to the card issuing bank 19a. At that point, each transaction is posted to the appropriate individual cardholder's account.

Detailed Description Text (39):
This off-line authorization method comprises use of an audio response unit ("ARU") 70, and a voice services department 72. The audio response unit 70 responds to dual tone multiple frequency (DTMF) signals provided by a merchant's standard TOUCH-TONE.RTM. telephone corresponding to the account number, expiration date and purchase amount for the proposed transaction. If the transaction is approved, the ARU's voice synthesizer provides an approval number as the authorization indicia, which the merchant manually enters into the terminal 35 via its keypad. In the preferred embodiment, the manually entered approval number is verified by logic in the terminal 35, to reduce mistakes and fraud.

Detailed Description Text (44):
FIG. 3 illustrates the preferred embodiment of a data card transaction processing terminal/printer system 30 constructed in accordance with the present invention. The terminal/printer system 30 comprises a transaction terminal 35, and a signature capture printer 38. The terminal 35 includes an injection molded plastic housing or case 101. A card swipe slot 103 is formed in the top portion of the case 101. When a card 15, such as a credit card, having a magnetic data stripe 110 is passed through the card swipe slot 103, the terminal 35 reads and decodes the data that is encoded in the card's magnetic stripe.

Detailed Description Text (45):
The preferred transaction terminal 35 also comprises an embossed card reader 112, comprising a tactile imager. When a card 15 having embossed characters 115 is inserted into the embossed card reader 112, the terminal 35 reads and decodes the account number embossed on the card. The embossed card reader 112 is located interiorly of a slot 113 in the housing 101, preferably opening toward the front of the terminal 35 for ease of access by a user.

Detailed Description Text (48):
According to the preferred embodiment of the invention, in the event the magnetic stripe 110 is damaged and unable to be read, the card will be placed in the embossed card reader 112 to detect the account number from the embossed area of the card.

Detailed Description Text (49):
According to other aspects of the invention, in the event the magnetic stripe 110 is damaged and unable to be read, the embossed card reader 112 may be used to detect the account number and, under certain circumstances, to restore the account number by utilizing at least a part of the account number read from the embossed area on the card, for the missing or defective account number, or portions thereof, read from the magnetic stripe.

Detailed Description Text (53):
More particularly described, for a transaction the terminal 35 first collects the card's account number and expiration date, and the proposed purchase amount. Once this data is collected, the signature capturing printer 38 prints the "header" portion of the receipt, which typically includes the date and time of the purchase, the account number, expiration date, purchase mount, and a line for the cardholder's signature. The printer then advances the paper until the line for the cardholder's signature is positioned over a signature capture window 160 located on the printer 38.

Detailed Description Text (61):
The terminal 35 further includes two RJ-11-type telephone connectors 212a, 212b labelled LINE and PHONE. The LINE 212a connector is used to connect a standard telephone line 48 to the terminal 35. In addition, there are two means by which a telephone or telephone handset may be connected to the terminal 35 in order to allow the terminal user to speak with a credit card processor or issuer. A standard telephone (not shown) may be connected to the PHONE connector 212b on the rear panel 201. Alternatively, a telephone handset 218 may be connected to an RJ-14-type telephone connector 220 located on the terminal's side panel. The handset 218 rests on the detachable cradle 223 when the handset is not in use.

Detailed Description Text (65):
The terminal circuit board 250 receives transactional data in four ways. Firstly, the keypad 120 provides means by which the operator may enter alphanumeric data and/or designate a specific operation for the terminal to perform. Secondly, the card swipe slot includes a magnetic read head 261 that allows the terminal 35 to detect the data encoded on both track 1 and track 2 of a data card. This analog signal is then amplified and conditioned by the card swipe interface circuit 265, before it is decoded by an I/O processor 270. Thirdly, an embossed card reader 112 employs tactile sensing elements to detect and decode the account number as represented by the embossed numerals located on a payment card. Fourthly, compressed signature signals are provided to the transaction terminal 35 from the signature capture printer 38 via a serial data link 145.

Detailed Description Text (93):
As will by now be understood, information contained on the magnetic stripe of a data card is read from the card in a transaction terminal 35 when a data card transaction is initiated. The information on the magnetic stripe 110 includes the card's account number, expiration date, and other information, in a format specified by ANSI Standard X4.16-1983. This standard is published by the American National Standards Institute, Inc., 1430 Broadway, New York, N.Y., and is incorporated herein by reference.

Detailed Description Text (100):
The output of the differentiating amplifier 495 is then connected to a zero crossing detector 497 that provides TTL level buffering for the signal and generates the F2FTRK1 signal at its output. Resistors R6 and R7 are connected between the output and non-inverting input of the zero crossing detector 497 in order to provide hysteresis as the voltage level changes at the input of the zero crossing detector 497.

Detailed Description Text (102):
As discussed more fury herein, the present invention is operative under certain circumstances to read the account number information from track 2 as an alternative source of information concerning the account number, expiration date, etc. In preferred embodiments of the invention, the terminal 35 may be made operative to restore defective or erroneous information read from track 1, in whole or in party, by substituting, in whole or in part, the account number and/or expiration date, to form a complete account number that satisfies the known account number checksum operations. This operation, in addition to providing a signal indicative that a card was physically present during a transaction, ensures that a complete account number can be obtained from the card, and cross .checked against the various sources of the account number information, as further checks on the accuracy of the account number and validity of the card.

Detailed Description Text (104):
As has been discussed in general earlier, preferred embodiments of the transaction terminal 35 include a tactile imager operating as an embossed card reader 112, shown in FIG. 9 and FIG. 10. The embossed card reader 112 is operative to tactilely

sense the raised or embossed characters on data cards and provide signals corresponding to the characters thereformed. These characters are then utilized to form an account number associated with the data card.

Detailed Description Text (105):
According to a preferred aspect of the present invention, the account number formed with the embossed card reader 112 is utilized as an electronically captured account number only when the account number cannot be obtained from reading the magnetic stripe on the card.

Detailed Description Text (106):
According to another aspect of the invention, the account number obtained from the embossed card reader may be used to restore a defective or erroneous account number, in whole or in part, by substitution of the account number, or selected characters thereof, where the magnetic stripe is damaged or is producing read errors. In yet another alternative embodiment, the data read from the embossed card reader may be used to compare against the account number obtained from the magnetic stripe as a further check on the validity of the card.

Detailed Description Text (110):
FIG. 9B illustrates the insertion of a card 15 into the slot 113 formed in the plastic terminal case 101. When a credit card 15 is completely inserted into the slot 113, it strikes a first switch actuating arm 515 positioned at the rear of the reader 112, causing it to move downwardly in the direction of arrow 516. The first switch actuating arm 515 pivots about an axis and its opposite end actuates a first switch 517a located on the control circuit 510, which produces a CARD INSERTED signal indicating that a card has been inserted into the embossed card reader.

Detailed Description Text (121):
As is more fully described in the above referenced patent, the electronics board 510 causes each of the rows to be strobed with an electrical pulse. As each of the rows is strobed, the device detects the signal present at each of the columns. The amplitude of the output voltage pulse is proportional to the capacitance, which is in turn proportional to the local force applied. Those skilled in the art will appreciate that the process employed in the present invention is analogous to those methods known in the an by which keyboards are polled. The signals thus detected are representative of the standard numeric characters formed in the embossed region 115 of the credit card 15, and may be decoded by the terminals I/O processor 270.

Detailed Description Text (123):
After strobing all rows of the imaging array 538, there will stored in an imaging array RAM associated with the I/O processor 270 as an array of digital signals corresponding to the raised and flat areas of the data card, comprising 1680 data elements or pixels. In the preferred embodiment, these data elements are then examined utilizing a simple "pattern recognition" algorithm to determine the identity of the characters forming the account number, by comparing the data in the imaging array RAM associated with the I/O processor 270 to patterns associated with the Farrington 7B characters stored in the Farrington character pattern ROM associated with the I/O processor 270. For example, data representing a single Farrington character comprises 9 words of 8 bits each, which are compared row by row to the rows of data elements stored in the imaging array RAM. It will thus be appreciated that storage of all Farrington characters (10 numerals) only requires 90 bytes.

Detailed Description Text (130):
Once a data card 15 is read by the embossed card reader 112, the 45 bits of data representative of the embossed region 115 are temporarily stored in random access memory associated with the I/O processor 270 until a complete account number is formed and provided to CPU 255.

Detailed Description Text (136):
It should also be understood that the threshold of the number of matches also determines whether the characters read from the card are "acceptable", that is, generally within the specifications prescribed for embossed characters on data cards. Those skilled in the art will appreciate that the embossed characters on a credit card comply with the Farrington 7B standard. However, the resolution of the disclosed embossed card reader 112 does not allow determination whether the characters of the embossing are within the precision set forth in the Farrington 7B standard. Nonetheless, this resolution is sufficient to permit determination as to whether the characters are grossly out of proportion, size, alignment, spacing, etc., and can detect badly worn cards or certain fraudulent cards. Thus, the determination of whether the embossed characters are "acceptable" will vary with the resolution of the embossed card reader and the degree to which the transaction processor decides to set parameters of acceptability.

Detailed Description Text (139):
If at step 563 the I/O processor 270 determines that the last character decoded represented the end of the embossed character region 115 of the card, the method advances to step 567, whereupon the I/O processor 270 assembles each of the individual characters decoded to form an account number, and provides this number to the terminal's main CPU 255 for subsequent use.

Detailed Description Text (173):
Those skilled in the art will understand that the amount of data used to represent the cardholder's signature directly affects the amount of memory required to store the data related to each transaction, and the time required to transmit the data from the transaction terminal 35 to the transaction processor's host computer 40. The present inventors believe that the amount of memory required to store the signature data can be significantly reduced by storing each stroke as a starting coordinate and data indicating the change from each coordinate to the next. Thus, small changes between two coordinates may be represented by fewer bits than large changes between two coordinates.

Detailed Description Text (175):
In order to reduce the amount of data required to store each signature, the (X,Y) PAIRS 690 will include data in one of four formats, depending on the magnitude of the change between the previous point and the current point. Each of the four formats comprises a two-bit "type" code or identifier, followed by a string of bits corresponding to the type of change.

Detailed Description Text (176):
When there is no change in either the X- or Y- direction, the value 691, 692 of the, (X,Y) PAIR 690 pertaining to that direction will be represented by two bits, which indicate a "no change" type identifier. If the change in either the X- or Y-coordinate is only 1 pixel, the data will be represented by three bits--two bits indicate a "one pixel" change type identifier, with one bit indicating the direction of the change, plus or minus. Larger changes between two coordinates will be stored in formats requiring six or nine bits. Thus, it will be understood that the data represented by the (X,Y) PAIRS 690 will be 2, 3, 6, or 9 bits long, and will cross byte (i.e., 8-bit) boundaries. Each of the four formats or types is described below in TABLE I:

Detailed Description Text (177):
Once the signature data is encoded in the above-described compressed format by the printer CPU 580, it is transmitted to the terminal 35 as serial data. At that point, the signature data is used to process the proposed credit transaction along with the other data collected by the terminal. In the preferred system 25 (illustrated in FIG. 2), the signature data (compressed signature signals) are stored by the merchant's transaction processor 12.

Detailed Description Text (188):
At step 742 the printer CPU determines the difference between the first coordinate position signal "A" and the second coordinate position signal "B", inasmuch as it has now been determined that there is a change in position of the stylus. As was described above, the data format representative of the change between the points "A" and "B" is determined by the difference between the two points. Thus, this method is operative to form the data denominated (X, Y) PAIRS 690 by determining the magnitude of the change for each coordinate X and Y for the data pair "A" and "B", and assigning the appropriate code as set forth above in TABLE I.

Detailed Description Text (205):
At step 817, the decompressor 42 clears a pair counter PRCNTR, and proceeds to step 820, where the decompressor reads the first (X,Y) pair 690a. Once the (X,Y) pair is read, the method is operative at step 822 to cause a line to be drawn between the starting point P1 and the point represented by the (X,Y) pair, which is P2. In the example, the X element 691 of the (X,Y) pair 690 is 00, thus indicating that there is no change in the X coordinate. The Y element 692 is 011, indicating that the second coordinate is (-1) from the first coordinate. Thus, the second point, which is labeled P2 in FIG. 23, is directly above the first coordinate P1.

Detailed Description Text (213):
an a bit code if there is no change in the respective coordinate between the first (X,Y) pair and the second (X,Y) pair;

Detailed Description Text (214):
a b bit code if there is a change of g picture elements in the respective coordinate between the first (X,Y) pair and the second (X,Y) pair;

Detailed Description Text (215):
a c bit code if there is a change of between g+1 and h picture elements in the respective coordinate between the first (X,Y) pair and the second (X,Y) pair; and

Detailed Description Text (216):
a d bit code if there is a change of between h+1 and i picture elements in the respective coordinate between the first (X,Y) pair and the second (X,Y) pair.

Detailed Description Text (227):
Likewise, the chargeback protection flag is operative to indicate that the merchant has engaged the transaction processor to provide transaction processing services that include the chargeback protection services. However, unlike the signature capture flag and the embossed data reader flag, a separate chargeback protection flag exists within the terminal for each of the credit cards that may be accepted by the terminal. Thus, it is possible for the transaction processor to provide chargeback protection to a merchant in conjunction with some specified data cards, and to provide conventional transaction processing services to the same merchant with respect to other data cards.

Detailed Description Text (228):
Those skilled in the an will understand that the terminal parameters uniquely configure the terminal. As a result, the terminal parameters, in conjunction with a specific transaction, are operative to determine the specific data that are sent to the transaction processor host computer during a credit card processing transaction. In the preferred terminal, the state of the embossed reader flag and chargeback protection flag, in conjunction with the nature of the data used to process the transaction, determine whether a "guarantee" or "transaction protected" flag is set when the transaction data is sent to the host for processing. The presence of the transaction protected flag indicates that the transaction data relates to a transaction that is chargeback protected.

Detailed Description Text (235):

The transaction processor may elect, at its option, to continue to provide chargeback protected transaction processing services to merchants in the event of a failure of the embossed card reader for the benefit of its merchants/customers, although doing so will require that the merchant enter card identifying data manually in the event the card swipe fails. This aspect of the present invention is described more completely in conjunction with FIG. 28.

Detailed Description Text (242):
If at step 853, the terminal determines that the proper parameters are resident in the terminal and that a download is not required, the method 850 branches to step 862, whereupon the terminal enters the main loop or idle state. Those skilled in the art will understand that it is from this main loop that the terminal may be instructed to carry out any of a variety of functions. For example, from the main loop, the terminal may be instructed to initiate, for example, a credit sale authorization transaction 900. A credit sale authorization transaction 900 is initiated when a magnetic card 15 is swiped through the swipe slot 103, or by the activation of one of the buttons on the terminal's keypad 120. The credit sale authorization transaction 900 is discussed more completely below.

Detailed Description Text (243):
In addition to the methods associated with the completion of a credit sale transaction, those skilled in the art will understand that both the preferred terminal and other prior an terminals are capable of performing a close terminal routine 932. Generally described, a close terminal routine is performed at predetermined intervals, and comprises steps wherein the terminal transmits all data related to transactions occurring during a predetermined accounting period to the transaction processor.

Detailed Description Text (246):
FIG. 26 illustrates a method 900 that is executed by the preferred terminal/printer 30 during an exemplary credit sale authorization transaction. The method 900 is preferably implemented as program steps for the terminal CPU 255.

Detailed Description Text (247):
This exemplary credit sale authorization transaction is carried out within the context of the preferred data card transaction system 25 constructed in accordance with FIG. 2. Such an exemplary credit sale is processed with transaction data capture by the terminal/printer 30, with authorization from an authorization source such as a host computer 40, and subsequent transmission of transaction data including compressed signature signals to the host 40. (It should be understood that while the host computer 40 in FIG. 2 is providing both authorization functions and transaction data processing functions, the authorization system and the transaction data processing system could be separate and independent systems.)

Detailed Description Text (248):
A credit sale authorization transaction is selected when the merchant desires to authorize a transaction and capture the transaction data simultaneously. When the transaction is authorized by the host computer 40, the transaction data will be captured by both the terminal 35 and the host computer 40. The method 900 is operative to insure that the data card is present, that the proper transaction data is collected and retained, and that the transaction qualifies for chargeback protection.

Detailed Description Text (249):
In FIG. 26, the method 900 begins at step 901 when a credit sale authorization transaction is initiated by the merchant, in response to presentation of a data card by a cardholder in connection with a proposed transaction. This typically occurs when a credit card 15 is swiped through the card swipe slot 103. At this step, a transaction record for the transaction, in which transaction information is stored for subsequent transmission to the host computer 40, is created. It will be

understood that the transaction record will include the transaction protected flag set in accordance with the state of the chargeback protection flag (CPF). The state of the transaction protected flag can also be conditioned upon whether or not an authorization has been received, as well as the nature of the authorization indicia received (such as whether the authorization indicia is electronic authorization or off-line authorization), at the discretion of the transaction processor.

Detailed Description Text (251):
If the card is not present at the time of the transaction, as would be the case in the event of a mail order or telephone order (MOTO) transaction, the merchant may manually enter the account number from the keyboard and complete the transaction. However, a MOTO transaction, where the card is not present, will not be chargeback protected (i.e., the transaction protected flag is cleared) since the evidence indicative of the validity of the transaction (e.g., the card is physically present and a signature is captured) is simply not available. Such transactions, being of a conventional nature, will not be discussed any further.

Detailed Description Text (252):
At step 905, a subroutine 905 denominated READ CARD DATA is executed. The READ CARD DATA subroutine 905 determines the account number and expiration date of the credit card. Generally, the preferred method attempts to reduce the likelihood of chargebacks by reading the account number and expiration date from the most reliable source available, which is usually the magnetic stripe. Thus, the READ CARD DATA subroutine 905 first attempts to read the account number and expiration date from the card's magnetic stripe. If reading the magnetic stripe is unsuccessful, the terminal prompts the merchant to insert the card into the embossed card reader 112 by displaying a message on the LCD 123. Once the card is inserted into the embossed card reader, the terminal 30 attempts to read the account number from the characters that are embossed on the card. The READ CARD DATA subroutine 905 is discussed in more detail in connection with FIG. 28.

Detailed Description Text (254):
Subsequent to execution of the READ CARD DATA subroutine 905, the terminal/printer 30 performs steps to determine whether the account number associated with the card is valid (with the known checksum calculation) at step 907, whether the card type is one that may be accepted by the merchant (i.e., whether the terminal accepts a given issuer's card) at step 911, and whether the card has expired at step 913. If any of the steps 907, 911, 913 result in a negative answer, the transaction will be terminated and the subroutine will return to the idle state in FIG. 25 (the main loop).

Detailed Description Text (255):
Once the account number and expiration date are determined to be valid, the method 900 proceeds to step 918. At step 918, the INPUT AMOUNT subroutine is executed. Generally described, the INPUT AMOUNT subroutine 918 prompts the merchant to enter the proposed purchase amount with the keyboard 120. The purpose of the subroutine is to obtain a proposed purchase amount from the merchant and to return that value.

Detailed Description Text (257):
After collecting the account number, expiration date, and proposed purchase amount, the terminal/printer 30 executes step 921, whereupon the signature capture printer 38 prints a portion of the sales receipt, typically a header portion. The portion of the receipt that is printed includes the date and time of the purchase, the account number, expiration date, purchase amount, and a line for the cardholder's signature. The signature capture printer 38 then advances the paper until the line for the signature is positioned over the signature capture window 160 located on the signature capture printer 38.

Detailed Description Text (262):

Once the terminal stores the data, the credit sale authorization transaction routine 900 is complete and returns control to the main loop or idle state in FIG. 25, awaiting further transactions.

Detailed Description Text (265):
Individual card issuers have historically been responsible for payment of transactions accompanied by evidence of a card presented in connection with the transaction, with a check-digited account number containing an identifying prefix assigned to them by a card issuing association.

Detailed Description Text (266):
In an effort to reduce fraudulent uses of account numbers, card associations began requiring encoding of information on the back of the plastic card (via a magnetic stripe) as well as embossing of the front of the card. Present day data cards include a plurality of tracks on the magnetic stripe, generally referred to as "track 1" and "track 2". Originally, only track 2 of the magnetic stripe was required to be encoded with information. Accordingly, prior art terminals were created with the ability to read only information in track 2 of the magnetic stripe.

Detailed Description Text (268):
Card association regulations allow some protection for transactions where "proof" that the account number was electronically read (rather than manually entered) can be provided (i.e., indicators that the authorization request has been generated from the magnetic stripe data), or alternatively where an impression (imprint) of an embossed card can be produced to "prove" that a card bearing the account number was actually presented for payment. Chargeback protection is limited to certain disputes regarding the validity of the account number, and issuers can obtain "counterfeit" loss protections for items paid on counterfeited cards.

Detailed Description Text (271):
As previously mentioned, many data cards nowadays include more than one track of information on the magnetic stripe. These multiple tracks contain redundant information, for example, both track 1 and track 2 contain the account number and expiration date, that could be used in the event of a failure to be able to read one of the tracks. Moreover, the embossing on the card contains the account number and expiration date. It would be desirable to be able to utilize these other sources of information of the account number, expiration date, etc. in the event of errors in reading the information from the magnetic stripe, for example if only a portion of the magnetic stripe were damaged. Alternative embodiments of the present invention allow such operation.

Detailed Description Text (272):
Transaction processors and others may therefore find it advantageous to utilize embodiments of the present invention that are operative to obtain information from one track or from the embossed card reader to construct a complete or error-corrected account number, expiration date, or the like in the event that an error occurs in reading another track of the magnetic stripe data. However, it will be understood that the preferred embodiments of the invention are constructed to obtain the desired information from the magnetic stripe.

Detailed Description Text (274):
In track 1 1001, data characters are encoded as six bit values, with one parity bit, for a total of seven bits per character. The major components or fields included in the track 1 data are an account number region, an account holder's name region, an expiration date region, and a longitudinal redundancy check (LRC) region. In addition, track 1 includes a start sentinel (SS), a format code (FC), a plurality of field separators (FS), discretionary data, and an end sentinel (ES). Those skilled in the art will also understand that the track 1 data illustrated in FIG. 27 are both preceded and followed by a series of clocking characters (logic

0's) that are read by the magnetic stripe read circuitry and used solely for the purpose of synchronizing the decode circuitry.

Detailed Description Text (275):
Track 2 1002 contains data characters that are encoded as four bit values, with one parity bit, for a total of five bits per character. The major components or fields included in the track 2 data are an account number region, an expiration date region, and an LRC region. In addition, track 2 data also includes a start sentinel (SS), a field separator (FS), discretionary data, an end sentinel (ES), and a series of leading and trailing clocking characters like those discussed in conjunction with track 1 1001.

Detailed Description Text (276):
The account numbers and expiration dates that are encoded on track 1 1001 and track 2 1002 are identical to each other and to the embossed account number and expiration date that appear on the face of the data card. Each track 1001, 1002 has a unique LRC that allows the terminal to verify the accuracy of the data read from the card. Generally described, the bit configuration of the LRC characters are identical to the bit configuration of the data characters. Thus, the LRC of track 1 1001 consists of seven bits including one parity bit, and the LRC of track 2 1002 consists of five bits including one parity bit. The LRC character recorded on each track is calculated so that a total number of ONE bits encoded in the corresponding bit location of all characters of the data message, including the start sentinel, data, end sentinel, and LRC characters, is even. The LRC character's parity bit is calculated so that the total number of ONE bits in the LRC character, including the parity bit, is odd.

Detailed Description Text (279):
Those skilled in the art will appreciate that it is possible with the present invention to restore the data read from the magnetic stripe in the event the LRC calculated by the terminal for the data read does not match that stored on the magnetic stripe. Even if the LRC for track 1 or track 2 indicates that the magnetic stripe read contained errors, it is possible that the account number was read properly, in whole or in part. By obtaining at least a portion of the account number from another source, such as the other track of the magnetic stripe or from the embossed card reader, replacing selected characters of the account number which may be in error with corresponding characters from the alternative source account number, and verifying the account code checksum, the account number may be restored to its original error-free state.

Detailed Description Text (280):
In the preferred embodiment, each character of the account number that is read by the embossed card reader 112 may be converted into the appropriate character format for track 1 or track 2 data, and used to restore at least a portion of the account number read from the magnetic stripe. Likewise, since each character in the account number of track 1 and or track 2 includes parity bits, it may be possible to identify which one of the plurality of alphanumeric characters forming the account number or expiration date is erroneous.

Detailed Description Text (281):
It is thus possible with the present invention to (1) identify a character or characters in the data read from a first track of the magnetic stripe that have incorrect parity, and substitute the corresponding character from a second track of the magnetic stripe or from the embossed card reader, or (2) substitute the entire account number or other data read from a first track with data read from a second track, or from the embossed card reader, and (3) thereafter recalculate the value for the checksum associated with the account number and/or LRC for the entire track to determine if it then matches the account number checksum and/or the LRC for the entire track.

Detailed Description Text (282):
If the checksum and/or LRC calculated from the account number formed by substituting selected characters or by substituting the entire account number, matches the account number checksum and/or LRC associated for the respective track, it will be determined that the data originally read from the particular track of the magnetic stripe was erroneous, that the error has been corrected, and that the accuracy of the account number, expiration date, etc. data has been verified by recalculating the checksum and/or LRC. By this method, it is possible to utilize data from any of the three sources to determine the account number and expiration date and to maintain a high level of confidence as to the accuracy of those numbers.

Detailed Description Text (284):
Turning now to FIG. 28, the preferred subroutine READ CARD DATA 905 will be described. This subroutine comprises steps taken in the preferred terminal for automatically reading the account number and expiration date from the card, and verifying the accuracy of the data to the extent possible. Namely, the READ CARD DATA subroutine 905 first attempts to read the account number and expiration date from a card's magnetic stripe. If the LRC is verified and the data appears to be accurate, the transaction is processed using that information. If the LRC verification fails and the magnetic data therefore is determined to be inaccurate, the subroutine reads and decodes the account number from the characters that are embossed on the face of the card, and prompts the merchant to manually enter the expiration date from the keyboard. This data is then used to restore portions of the data read from the magnetic stripe and the LRC is recalculated. If the LRC is verified, the transaction is processed using the restored magnetic data. However, if the attempt to verify LRC fails again, the transaction is processed using the account data that was read from the embossed characters.

Detailed Description Text (286):
At step 1022, the CPU 255 calculates LRC values for the data read from both tracks 1 and 2, and compares them to the LRC values encoded on the card's magnetic stripe. If the data from either track is determined to be valid, the method proceeds to step 1025. If neither track 11001 nor track 2 1002 is valid, the subroutine proceeds to step 1027 and the merchant is prompted to swipe the credit card 15 through the card swipe slot 103 again, by displaying the message "CARD NOT READ--PLEASE SWIPE CARD AGAIN" on the LCD 123 on the terminal. When the card 15 is swiped through the card swipe slot 103 the second time, the preferred card swipe interface 265 again attempts to read and decode the data recorded on both track 1 1001 and track 2 1002 of the card's magnetic stripe 110.

Detailed Description Text (288):
At step 1025, the terminal determines whether the track 1 data possessed a valid LRC. If so, the track 1 data is determined to be valid, and the CPU proceeds to step 1032. At step 1032, a flag is set to indicate that the data used to process the transaction is "swiped track 1 data" and the CPU 255 exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION routine 900.

Detailed Description Text (289):
Returning now to step 1025, in the event the track 1 data is determined to be invalid, the terminal proceeds to step 1035, where the track 1 account number is compared to the track 2 account number. If the account numbers read from track 1 and track 2 are different, the CPU 255 proceeds to step 1037 and begins the process of using the account number read from track 2 to restore the data read from track 1. If the account numbers are found to be identical, at step 1035, the method 905 advances to step 1045, which is discussed below.

Detailed Description Text (290):
Those skilled in the an will understand that even though track 1 and track 2 both include the account number and expiration date, it is preferable to process a

transaction using track 1 data if possible, since it includes the cardholder's name and additional discretionary data. In addition, the track 1 discretionary data may include alphanumeric characters, whereas all track 2 is limited to numeric data.

Detailed Description Text (291):
At step 1037, the defective track 1 data 1001 is restored by substituting at least a portion of the account number from track 2 into the account number field of track 1. With the track 1 data reconstructed in this manner, the terminal proceeds to step 1040 and attempts to verify the validity of the restored track 1 data by retesting the LRC. If the LRC is determined to be valid, the terminal proceeds to step 1032 whereupon it sets a flag to indicate that the data used to process the transaction is "swiped track 1 data built using track 2", exits the READ CARD DATA subroutine 905, and returns to the CREDIT SALE AUTHORIZATION method 900.

Detailed Description Text (292):
If, at step 1040, the reconstructed track 1 data is determined to be invalid, the terminal proceeds to step 1047. At step 1047, the terminal sets a flag indicating that the data used to process the transaction is "swiped track 2 data", exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900.

Detailed Description Text (293):
Turning now to step 1045, if the track 1 and track 2 expiration dates are determined to be different, the program advances to step 1050. At this step, the terminal attempts to restore the data read from track 1 by replacing the track 1 expiration date with the expiration date read from track 2. The method 905 then returns to step 1040, where the terminal recalculates the track 1 LRC and tests the validity of the restored track 1 data. If the restored track 1 data is now valid, the terminal proceeds to step 1037, whereupon the program sets a flag to indicate that the data used to process the transaction is "swiped track 1 data built using track 2", leaves the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900.

Detailed Description Text (294):
If, at step 1040, the reconstructed track 1 data is determined to be invalid, the terminal proceeds to step 1047. At step 1047, the terminal sets a flag indicating that the data used to process the transaction is "swiped track 2 data", exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900.

Detailed Description Text (295):
Returning now to step 1030, the preferred steps executed in the event neither track 1 nor track 2 are valid will be described. If, at step 1030, neither track 1 nor track 2 are determined to be valid, the program advances to step 1055, and determines whether the embossed card reader 112 is activated. If so, the terminal proceeds to step 1057. If the terminal's embossed card reader is not activated, the program proceeds to step 1084 and allows the merchant to manually enter the account number and expiration date. This process is described more completely below.

Detailed Description Text (296):
At step 1057, the terminal first causes the liquid crystal display 123 to display a message instructing the merchant to insert the card 15 into the terminal's embossed card reader 112, for example "INSERT CARD INTO EMBOSSED CARD READER". Once the card is inserted, the embossed card reader 112 automatically reads and decodes the numeric characters 115 that are representative of the account number and embossed on the face of the card.

Detailed Description Text (297):
Once the embossed characters are read, the program proceeds to step 1060, and determines whether the characters read-from the card are "acceptable", that is,

generally within the specifications prescribed for embossed characters on data cards. Those skilled in the art will appreciate that the embossed characters on a credit card comply with the Farrington 7B standard. However, the resolution of the disclosed embossed card reader 112 does not allow determination whether the characters of the embossing are within the precision set forth in the Farrington 7B standard. Nonetheless, this resolution is sufficient to permit determination as to whether the characters are grossly out of proportion, size, alignment, spacing, etc., and can detect badly worn cards or certain fraudulent cards. Thus, the determination of whether the embossed characters are "acceptable" will vary with the resolution of the embossed card reader and the degree to which the transaction processor decides to set parameters of acceptability. For purposes of the present invention, characters are acceptable if the size and spacing of the characters is within the tolerance of the tactile imager, that is, about 0.5 millimeters.

Detailed Description Text (299):
In addition to determining whether the embossed characters themselves are acceptable at step 1060, the terminal also tests to see if the data from the embossed card reader is all numeric, if the length of the account number is valid for the card type, and if the account number passes the MOD 10 check, that is, the known checksum calculation associated with credit card account numbers. If any of these tests fail, the characters read by the embossed card reader is determined to be not acceptable.

Detailed Description Text (301):
At step 1062, the terminal causes the liquid crystal display 123 to instruct the merchant to enter the expiration date via the keyboard 120. Once the merchant has read the expiration date from the credit card and entered it from the keypad, the program goes to step 1064. At this step, the terminal determines whether it was able to read any data from the magnetic stripe at the previous steps 1020, 10:17. If the terminal determines that the magnetic data was nonexistent, the program advances to step 1066, whereupon the terminal sets a flag indicating that the data used to process the transaction is "embossed data only". The terminal then exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900.

Detailed Description Text (303):
If, at step 1064, the terminal determines that magnetic track data does exist, the program proceeds to step 1068. At this step, the terminal reconstructs the data read from track 1 by replacing the account number and expiration date from track 1 with the account number read by the embossed character reader 112 and the expiration date that was manually entered by the merchant. Once the reconstruction is complete, the program proceeds to step 1070, and recalculates the LRC for the restored track 1 data. If the LRC is verified and the restored track 1 data is determined to be valid, the terminal proceeds to step 1072, where it sets a flag indicating that the data used to process the transaction is "embossed data inserted into track 1", exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900. If the reconstructed track 1 data is invalid, the program goes to step 1074.

Detailed Description Text (304):
At step 1074, the terminal reconstructs the track 2 data by replacing the account number and expiration date read from track 2 with the account number read by the embossed character reader 112 and the expiration date entered by the merchant. Once the reconstruction is complete, the program proceeds to step 1076, and recalculates the LRC for the restored track 2 data. If the LRC is verified and the restored track 2 data is thus determined to be valid, the terminal proceeds to step 1078, where it sets a flag indicating that the data used to process the transaction is "embossed data inserted into track 2". The terminal then exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900. If the reconstructed track 2 data is invalid, the program goes to step 1080.

Detailed Description Text (305):
At step 1080, the terminal sets a flag indicating that the data used to process the transaction is "track 1 or track 2 data with embossed data inserted and LRC failure". The program then exits the READ CARD DATA subroutine 905 and returns to the CREDIT SALE AUTHORIZATION method 900.

Detailed Description Text (306):
Returning now to step 1060, the steps that follow a determination that the characters read by the embossed character reader are not acceptable will be described. If the embossed characters read from the card are not acceptable, the program proceeds to step 1082 and determines whether the embossed card reader 112 is broken. If not, the terminal advances to step 1088 and causes the liquid crystal display 123 to instruct the merchant to request another form of payment from the customer. The credit sale transaction is then terminated.

Detailed Description Text (307):
If the embossed card reader 112 is determined to be inoperative at step 1082, the program proceeds to step 1083, where it causes the liquid crystal display 123 to direct the merchant to notify the transaction processor 12 that the embossed card reader appears to be defective. Once notified, the transaction processor will cause the terminal software to be modified temporarily to allow the terminal to continue processing credit sales until the embossed card reader can be repaired or replaced. The program then proceeds to step 1084 where it allows the merchant to manually enter the account number and expiration date. Once the account number and expiration date are manually entered by the merchant, the terminal proceeds to step 1086, where it sets a flag indicated that the data used to process the transaction is "manually entered", exits the READ CARD DATA subroutine 905, and returns to the CREDIT SALE AUTHORIZATION method 900. Again, it will be understood that transaction processors and credit card issuers may not afford the same treatment to transactions flagged as "manually entered" as they would to magnetically read transactions.

Detailed Description Text (308):
An alternative embodiment of the present invention contemplates additional verification of the authenticity of the account number read from the card. For example, a terminal constructed according to an alternative embodiment contemplates that the credit sale transaction would be terminated if the terminal is unable to read the data from the card's magnetic stripe. In addition, once the data is successfully read from the magnetic stripe, the terminal prompts the merchant to insert the card into the embossed card reader or to manually enter the account number via the keyboard so that the magnetically read account number can be verified against the number obtained manually or read from the embossed card reader. In this manner, a transaction processor is enabled to receive additional assurance that a card is genuine and that the embossed characters and/or magnetic stripe have not been altered by the cardholder.

Detailed Description Text (309):
From the foregoing, those skilled in the art will understand and appreciate that the "restoration" of data which has a redundant source is an option available with use of the present invention. It will be appreciated that one method of restoring data involves reconstructing the account number and/or expiration date read from a first track with data read from a second track and/or the embossed card reader. Another common use would be to restore either track's data with data read from the embossed card reader. In any case, preferred embodiments of the present invention will identify the manner of obtaining the data and transmit information corresponding thereto, such as "embossed data inserted into track 1", "embossed data inserted into track 2", "track 2 data inserted into track 1", "track 1 or track 2 data with embossed data inserted and LRC failure", and the like.

Detailed Description Text (313):
As described earlier, the portion of the receipt printed at step 921 of the method 900 (FIG. 26) includes the date and time of the transaction, purchase amount, credit card account number and expiration date. After the information recorded on the receipt is verified, the cardholder signs the receipt over the signature capture window 160 on the signature capture printer 38 using the magnetic/ink stylus 165.

Detailed Description Text (317):
Once the data is compressed, the compressed data representative of the signature is transferred from the signature capture printer 38 to the preferred terminal 35 at step 1115. Once the facsimile of the signature is received by the terminal, the method 923 proceeds to step 1117, where the terminal exits the subroutine 923 and returns to the CREDIT SALE AUTHORIZATION method 900 in FIG. 26.

Detailed Description Text (319):
FIG. 30 illustrates the method that is embodied in the REQUEST AUTHORIZATION subroutine 926, which is executed by the terminal 35. Generally described, the method 926 causes the terminal 35 to initiate communications with the host computer 40 of a transaction processor. During the established communications session, the terminal transmits the data pertaining to the proposed transaction and requests an authorization indicia or code from the host computer. The authorization will be granted if the card issuer or its agent so stipulates, or, in the event of failure to communicate with the card issuer or its agent, if the transaction data received by the host computer falls within predetermined parameters that are prescribed by the credit card transaction processor 12 or by the card issuing association 18a-d.

Detailed Description Text (320):
In the event the terminal 35 is unable to establish communications with the host computer 40, or communications are interrupted, the terminal then attempts to initiate and receive an off-line authorization from an alternative facility known as an audio response unit (ARU) 70. If the transaction is not approved by one of these two means, the transaction is terminated. However, if the transaction is authorized, the subroutine causes the authorization number to be stored and the routine terminates and returns to the CREDIT SALE AUTHORIZATION routine 900.

Detailed Description Text (329):
In the event that communications with either the primary authorization source or the secondary authorization source have been established, at step 1160 the program causes the transaction data accumulated by the terminal to be transmitted to the host computer. Once the account number, expiration date, purchase amount, transaction date, and compressed signature signals are transmitted to the host computer 40, the program proceeds to step 1162. Such a transmission comprises a request for authorization of the transaction.

Detailed Description Text (330):
It will be appreciated here that the described method of transmitting to the host all transaction data (account number, expiration date, purchase amount, transaction date, compressed signature signals, and transaction protected flag) upon establishment of communications for purposes of seeking an authorization is presently preferred for use in the present invention. Nonetheless, those skilled in the art will appreciate that other sequences of operation are considered within the scope of the present invention. For example, alternative embodiments of the present invention contemplate operation wherein the authorization is sought immediately after obtaining the account number, and wherein the compressed signature signals are transmitted after obtaining the authorization. However, it will be appreciated that for transaction processors electing to provide chargeback protection on behalf of merchant/customers, it is advantageous to capture all relevant information concerning the transaction including the signature prior to seeking authorization.

Detailed Description Text (331):
At step 1162, the program receives a response from the host computer in response to the authorization request. If at step 1164 the response is a "decline", the subroutine exits and control is returned to the CREDIT SALE AUTHORIZATION routine 900. If the response was not a decline, the inquiry is made at step 1166 whether the response was an approval.

Detailed Description Text (332):
If the response was an approval, the program branches to step 1170, where the approval code is recorded within the terminal's memory associated with the other transaction data. The approval code will be retained with the other transaction data until the terminal is closed, in accordance with the CLOSE TERMINAL subroutine. The subroutine exits and control is returned to the CREDIT SALE AUTHORIZATION routine 900.

Detailed Description Text (340):
If automatic DTMF transmission of transaction data is not selected, the merchant will enter the account number, expiration date, and purchase amount using the portion of the keyboard 120 that forms a telephone-type keypad. Once the audio response unit 70 receives the transaction data, the ARU automatically attempts to obtain an authorization approval from the card issuer via its connection to an appropriate authorization source, or, in the event of a host outage, determines whether the transaction may be approved according to predetermined guidelines for off-line authorizations maintained by the transaction processor 12. If so, the ARU produces an audible series of numbers corresponding to an off-line authorization number. If the transaction may not be approved, the ARU will automatically refer the call to a live operator in the voice services department 72 (FIG. 2) in order to accommodate a direct voice telephone call to the card issuer.

Detailed Description Text (342):
At step 1180, the inquiry is made whether an approval was received from the ARU 70. If not, the terminal branches to step 1182, where the inquiry is made whether the response to the authorization request was a decline. If the response was a decline, the at step 1184 the terminal displays "DECLINE" on the LCD 123 and the subroutine exits and control is returned to the CREDIT SALE AUTHORIZATION routine 900. The merchant of course must at this juncture decide whether to proceed with the transaction using another source of payment.

Detailed Description Text (344):
At step 1193, a check is made whether the "charge back protection" (CPF) flag (described in TABLE II) has been set. If not, the subroutine exits to the CREDIT SALE AUTHORIZATION routine. 900.

Detailed Description Text (348):
Returning now to step 1182, if the response from the off line approval source was not a decline, it is deemed that the response is a "call me", and the program branches to step 1186. At this step, the merchant is advised via a message on the LCD 123 to call the card issuer for an approval or other message. In alternative embodiment, the terminal may be programmed with the telephone number of the card issuer and the terminal will be automatically operative for initiating a call to the issuer. After calling the card issuer, the program branches to step 1188 and transmits any required data to the card issuer, if applicable, and exits. Typically, in such cases the terminal will switch the telephone line to the handset, since a voice communication with a live operator associated with the card issuer will likely follow. Thus, in some cases the merchant may speak directly to a voice services operator. After step 1188, the subroutine exits and control is returned to the CREDIT SALE AUTHORIZATION routine 900.

Detailed Description Text (352):
The STORE DATA subroutine 930 begins at step 1202, where the terminal determines

whether the authorization code received by the terminal at step 926 was an off-line authorization code. If it was not an off-line authorization, the method proceeds to step 1204, where the terminal's microprocessor 401 causes all data corresponding to the transaction, except the signature signals, to be retained in the terminal's memory 258. Memory formerly utilized for storing the signature associated with the transaction is then released for other uses by the microprocessor 401, including storage of other transaction data. Once the data is stored at step 1204, the program exits and returns to the CREDIT SALE AUTHORIZATION routine 900.

Detailed Description Text (353):
If, at step 1202 the authorization was determined to have been received via an off-line authorization code, the method advances to step 1206. At this point, the CPU 255 in the terminal causes all of the transaction data including the signature to be stored in the terminal's memory 258. Once the appropriate data is stored, the program exits and returns to the CREDIT SALE AUTHORIZATION routine 900.

Detailed Description Text (356):
Those skilled in the art will understand that in the present invention and in prior art data capture terminals, the transaction data is preferably transmitted to the transaction processor at the time of each transaction. Thus, it may only be necessary to transmit a total amount representing the merchant's accounts receivable from the transaction processor when the terminal is closed. However, there are times when the terminal is unable to communicate with the host computer, and terminals constructed in accordance with the present invention store all transaction data until it can be transmitted to the host computer 40 at the time the terminal is closed.

Detailed Description Text (363):
After the foregoing discussion, those skilled in the art will be enabled to construct a data card terminal/printer including a signature capture printer, with embossed card reader, having the ability to provide more information concerning a particular data card transaction than has heretofore been possible. Transaction processors will be able to enjoy the advantages provided by such a terminal/printer combination, or even merely certain subcombinations such as the signature capture printer, the restoration of unreadable or damaged data read from a first magnetic stripe track with data from a second magnetic stripe track or with data from the embossed card reader. Because of the additional confidence in the validity and collectability of a transaction afforded by use of the disclosed terminal/printer 30, it may be expected that transaction processors will be able to provide additional types of services on behalf of their merchant/customers, namely, the provision of chargeback protection for transactions conducted using the terminal.

Detailed Description Text (364):
Furthermore, a transaction processor, such as the transaction processor 12, that utilizes the present invention to capture and store the transaction data including signature signals on behalf of its customers/merchants will be able to provide valuable services on behalf of its customers. Such services include the retrieval of transaction data upon request of a card issuer or card issuing association, thereby eliminating any involvement of and inconvenience to the merchant, and by eliminating the need for the merchant to retain paper records of transactions.

Detailed Description Text (368):
Turning now to FIG. 33, a method 1400 that is employed by a transaction processor host computer 40 to process a retrieval request will be described. A system constructed in accordance with the present invention facilitates retrieval requests by providing a method for storing information corresponding to transactions, including the signature, in a compact electronic form. Merchants who retain the services of a transaction processor that uses systems constructed in accordance with the present invention will find that they no longer have the need to store paper records of their data card transactions, since such data is stored

electronically, paperlessly, in the database of the transaction processor. Transaction processors using the present invention can respond to retrieval requests on behalf their customers (e.g. merchants) quickly and efficiently since all data is stored in the transaction processor's host computer, allowing the transaction processor to provide a valuable service to the merchant.

Detailed Description Text (370):
Starting in FIG. 33 at step 1401, a transaction processor 12 receives a retrieval request from one of the card issuing associations 18a-d. This retrieval request contains certain identifying information such as a transaction reference number, cardholder account number, transaction date, and transaction amount. At step 1405, the host computer 40 of the transaction processor causes a receipt file stored in data storage 64 to be searched by the reference number (or other identifying information) contained in the retrieval request to locate a data item corresponding to the transaction in question. Once this data item, also considered a "receipt", is located, the method proceeds to step 1407.

Detailed Description Text (371):
At step 1407, the host computer causes a facsimile of the data item or receipt corresponding to the requested transaction to be printed by the transaction processor 12. Reproduction of the receipt generally involves printing all data associated with the transaction such as purchase amount, account number, expiration date, authorization number, merchant's product identifying or other inventory code, and cardholder signature. The cardholder signature of course is stored in its compressed form, so printing the receipt requires decompressing with the decompressor software 42 and reconstructing the strokes of the signature in the manner described in connection with FIG. 24.

Detailed Description Text (372):
Thus, the cardholder's signature is reproduced along with the other transaction data. The retrieved receipt is then printed at step 1407, and includes the reconstructed signature. At step 1409, the printed receipt containing the transaction data and signature is forwarded to the credit card issuing association or other entity that initiated the retrieval request.

Detailed Description Text (374):
Turning now to FIG. 34, a method 1500 that is employed by the transaction processor host computer 40 in the preferred system to process a chargeback will be described. Generally, the preferred method 1500 allows a transaction processor that utilizes terminals 30 and software constructed according to the present invention to respond to most chargebacks without the involvement of the merchant. This is possible because a system constructed in accordance with the present invention insures that all of the transaction data, including the cardholder's signature, is recorded and stored by the transaction processor 12 in a storage facility 64. Use of the present invention therefore allows a transaction processor to assume the risk of certain types of chargebacks on behalf of its customers (merchants) if it so chooses, with a high level of confidence that the transaction was a valid one.

Detailed Description Text (375):
Starting in FIG. 34 at step 1501, the transaction processor 12 receives a chargeback from one of the credit card issuing association 18a-d or from another source within the chain of data card transaction communications. The method then proceeds to step 1505, where the host computer 40 determines whether the a copy of the transaction receipt will be needed in order to respond to the chargeback. This would be the case when a cardholder initiates a chargeback because he or she believes there is a discrepancy in the transaction data. It will be appreciated that certain types of chargebacks may require documentation in accordance with card issuing institution regulations, while others may not.

Detailed Description Text (379):

At step 1519, the host computer determines whether the chargeback is related to a customer dispute. If so, the method advances to step 1522, where the dispute is researched and, if the dispute appears valid, the responsibility for the chargeback is transferred to the merchant. It will be recalled that a customer dispute chargeback typically arises when the customer (cardholder) denies participating in a transaction, or is dissatisfied with the goods or services purchased. When possible, the transaction processor will refute cardholder disputes by using information obtained by the terminal, i.e., the card present indicator and/or the cardholder signature. In other cases, the transaction processor can not assume the risk of the chargeback, since the transaction processor has no control over disputes that arose from a customer (cardholder) of the merchant. Thus, it will be left to the merchant to refute charges related to these disputes.

Detailed Description Text (380):
If, at step 1520 the chargeback is determined not to have arisen from a customer dispute, the method proceeds to step 1525. At this step, the transaction processor 12 absorbs the loss associated with the chargeback or re-presents the transaction data to the issuer.

Detailed Description Text (381):
It will be appreciated that use of the preferred terminal/printer 30 can provide a transaction processor with substantial assistance in connection with a cardholder or customer dispute mainly when the cardholder can be assuaged with a copy of the receipt bearing his or her signature, and is satisfied that the signature is authentically his or hers, or is reminded (for example by reviewing the date, merchant name and location, etc.) that he or she actually participated in the transaction in question.

Detailed Description Text (382):
It will also be appreciated that use of the present invention minimizes what may be termed "technical chargebacks" to a merchant, and allows a transaction processor to offer to assume the risk of such chargebacks provided that the merchant uses a terminal constructed in accordance with the present invention. Technical chargebacks often result from erroneous keying in of transaction data, such as the account number or purchase amount, by the merchant. While the preferred terminal cannot assist the merchant in keying in the proper purchase amount, when coupled with known bar code scanners, connected to one of the RS-232 serial ports 208 associated with the terminal 35, the terminal can minimize amount entry errors.

Detailed Description Text (383):
By ensuring that a card is present during every transaction (such as by verifying the account number read from a second track and/or the embossed card reader against a first track's account number), obtaining an authorization from an authorization source, bar code scanning the UPC codes to obtain purchase amounts, automatically computing taxes and other discounts, and requiring that a signature be obtained before a transaction will be accepted at the terminal, systems constructed in accordance with the present invention provide transaction processors and their customers/merchants with high levels of assurance that a given transaction will not be charged back because of keying errors or other technical reasons. Furthermore, since the same transaction data is used for the initial transaction capture, authorization, clearing (closing), and settlement, use of systems and terminals constructed in accordance with the present invention reduces keying errors and thereby further minimizes the likelihood of a technical chargeback.

Detailed Description Text (386):
Starting at step 1601, the program resident in the ARU 70 examines the number dialed (DNIS). Those skilled in the art will understand that many transaction processors utilize telecommunications services provided by private telecommunications firms (such as AT&T, US SPRINT, MCI, etc.) for connecting merchant terminals to their host systems. Such private telecommunications providers

have the ability to identify calls originating with certain merchants by virtue of the phone number dialed in order to access a particular incoming telephone line. This capability is called by those skilled in the art as "DNIS". Essentially, DNIS comprises information available to the ARU 70 concerning the number dialed by an incoming call on a particular telephone line. DNIS typically allows identification of a particular merchant or category of merchant (for example, one category of merchant may include large retailers conducting business from a number of stores through a centralized facility) that is a customer of the transaction processor 12, as well as determination whether a merchant has DTMF-capable telephone equipment or rotary dial equipment.

Detailed Description Text (391):
Returning to step 1607, if neither the number called nor the calling number is indicative of the merchant, the program will proceed to step 1613. At step 1613 the program causes the ARU to accept the sale amount and cardholder account number, if present in the form of DTMF signals from the terminal. In the event the data has not been presented by the merchant or by a data card terminal constructed in accordance with the present invention, with off-line transaction capability, the program will cause the ARU to request the data, one field at a time, where needed. If some data elements are already present, such as the merchant number, this field will not be requested. Similarly, individual fields may be re-requested in an iterative process if subsequent validation logic detects errors or omissions. The program then proceeds to step 1619.

Detailed Description Text (393):
At step 1621, the program checks each field for a variety of conditions, depending on the individual fields. Among these are field length, numeric content, reasonableness, and, in the case of a cardholder account number, check digit verification. If an error is found in any field, the program proceeds to step 1625 before proceeding to edit the next field.

Detailed Description Text (404):
At step 1681, the program calculates a check digit based on information that is already contained in the terminal, such as the account number, expiration date, purchase amount, transaction date, etc., and appends it to the end of the two-digit ARU response code, to form a three-digit approval code. The ARU response code thus formed is stored by the ARU in a manner that corresponds with the authorization indicia that was received from the authorization source, so that the authorization indicia may subsequently be associated with the transaction. The program then proceeds to step 1682.

Detailed Description Text (415):
Returning now to step 1632, if the authorization response received from the host computer was a "decline", the program then proceeds to step 1697. At step 1697, the program causes the ARU to speak a "decline" message of the currently preferred form, "Your customer's bank has declined this transaction", disconnect the call, and then exits. The form and content of this message may vary from time to time to accommodate the need for comprehension by the merchant.

Detailed Description Paragraph Table (2):
TABLE I _____ 00 No change from the previous coordinate. 01S A change of +/-1 pixel from the previous coordinate; S = 0 if positive; S = 1 if negative. 10SXXX A change of +2 to +9 or -2 to -9 pixels; S = 0 if positive; S = 1 if negative; (XXX + 2) = change from previous coordinate. 11SXXXXXX A change of +10 to +73 or -10 to -73; S = 0 if positive; S = 1 if negative; (XXXXXX + 10) = change from previous coordinate

---

CLAIMS:

3. The terminal of claim 1, further comprising:

means for detecting an account number associated with the data card presented by the cardholder in connection with the proposed transaction;

means for automatically providing said detected account number to said transaction processing host computer system or said ARU.

4. The terminal of claim 3, wherein said account number providing means comprises digital signal means for providing said detected account number to said transaction processing host computer system, and DTMF means for providing said detected account number to said ARU.

10. The method of claim 9, further comprising the steps of:

detecting an account number associated with the data card presented by the cardholder in connection with the proposed transaction;

automatically providing the detected account number to the transaction processing host computer system or the ARU.

11. The method of claim 10, wherein the step of automatically providing the detected account number comprises providing the detected account number by digital signals to the transaction processing host computer system and by DTMF tones to the ARU.

23. The terminal of claim 21, further comprising:

an account number reader operative for detecting an account number associated with the data card presented by the cardholder in connection with the proposed transaction;

a transmitter for automatically providing said detected account number to said transaction processing host computer system or said ARU.

24. The terminal of claim 23, wherein said transmitter utilizes digital signals for providing said detected account number to said transaction processing host computer system, and DTMF signals for providing said detected account number to said ARU.

Previous Doc Next Doc Go to Doc#

Web

Definitions of **cashback transaction** on the Web:

- A Transaction initiated with a Card at a POS Terminal and authorized from a Cash Account, in which the transaction amount debited against the Cardholder's Account is given to the Cardholder by the Merchant in whole or in part in cash.
  www.nacsonline.com/NACS/Resource/Technology/tech_080100_ir.htm

Web

Definitions of **cashback mortgage** on the Web:

- This is a mortgage in which the Lender refunds a sum of money, either as a percentage of the loan or a flat figure, to the borrower upon completion. With this type of offer the borrower will typically be tied to the Lender's SVR by early repayment charges necessitating repayment of the cashback if the loan is repaid within a set period.
  www.themortgageexplorer.co.uk/Mortgage_Glossary_Terms.htm

global investor Glossary

Cashback

Definition

A sales incentive, commonly used on mortgages, which gives customers a cash sum as soon as the deal is signed. Typically linked to heavy redemption fees.

See also

Redemption fees

Related books


The Wealth Equation by Peter J. Tanous

Everything You Need To Know About Money And Investing A Financial

Other terms in this category

Affinity cards ■ Affluenza ■ Annual bonus ■ Annual equivalent rate ■ Bancassurance ■ Base rate tracker mortgage ■ Basic state pension ■ Basic sum assured ■ Beneficial loan ■ Benefits in kind ■ Budget account ■ Buyers Guide ■ Cancellation period ■ Cap and collar rate ■ Capped rate mortgage ■ Carpetbagger ■ Cashback ■ Cat mark ■ Cat standard ■ Chargeable event